LTE Signaling Procedure

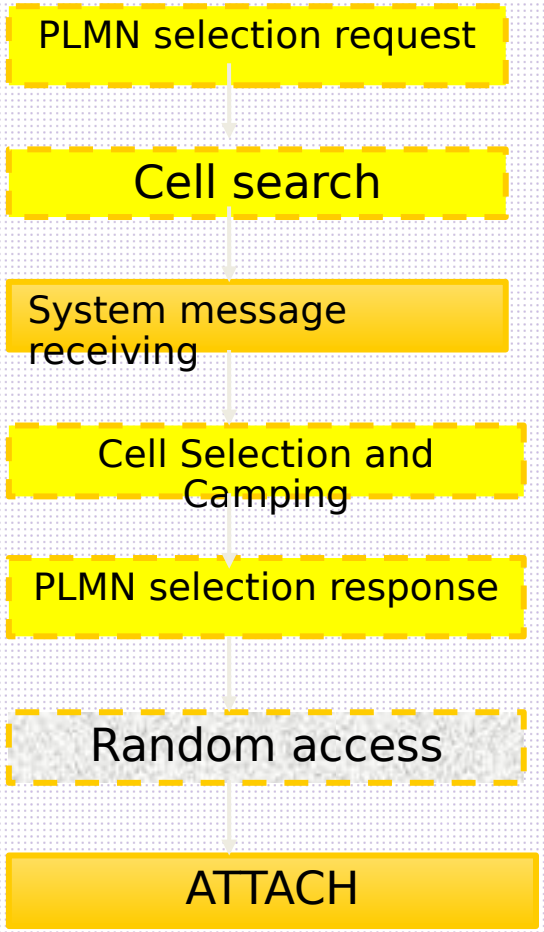
www.huawei.com

HUAWEI

Contents

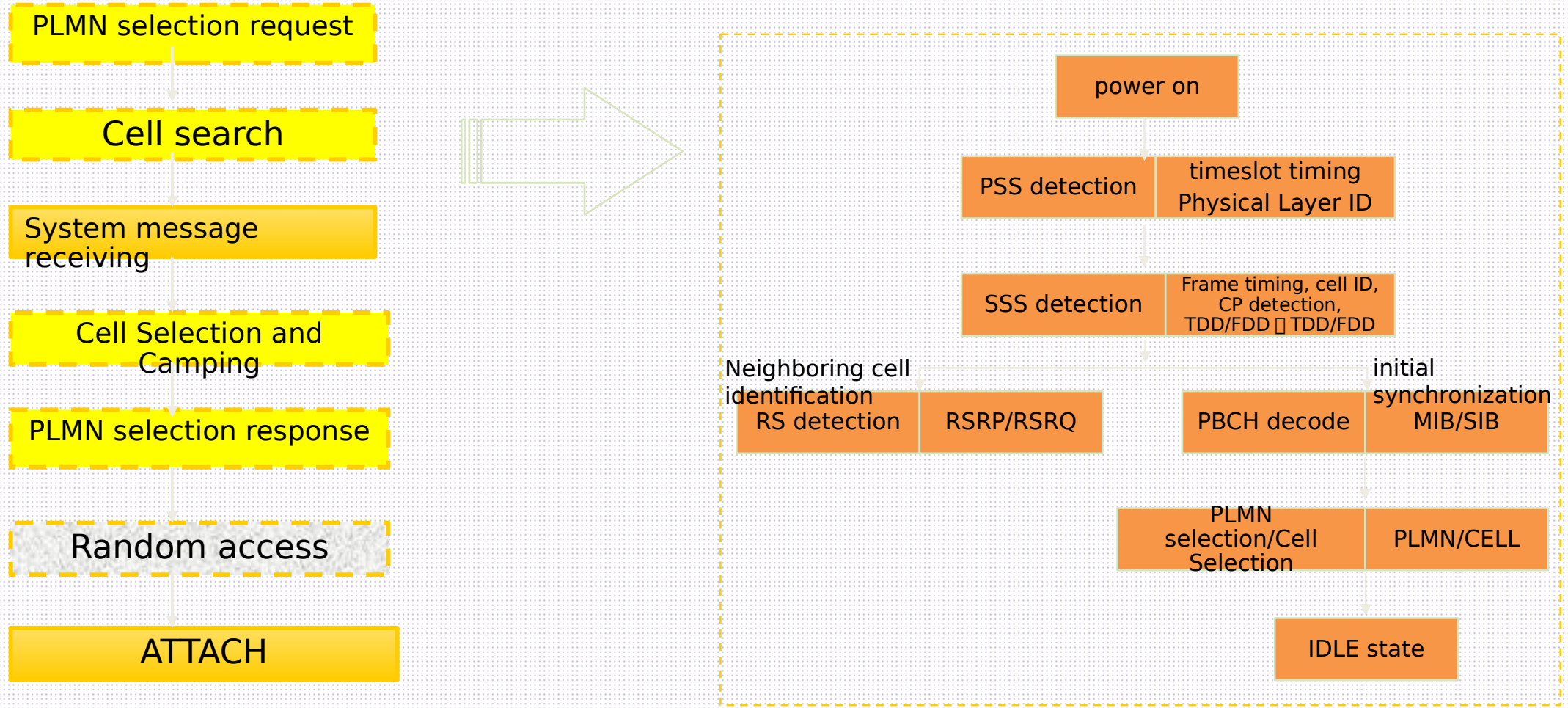
UE Power-on and Network Access Procedure

- **PLMN search (cell search)**：When the UE is powered on, its primary task is to find and contact the network. In essence, it is a downlink synchronization process.
- **System message receiving**：The subsequent admission and camping procedures can be performed only after Layer 2 and Layer 1 are configured.
- **Random access**：Eliminate contention between different UEs and achieve uplink synchronization.
- **Attach**：Establish the same mobility context between the UE and the MME and the default bearer between the UE and the PDN GW.T ttac e U address allocated by the network.
- **Common Processes**：Authentication process and security mode process.



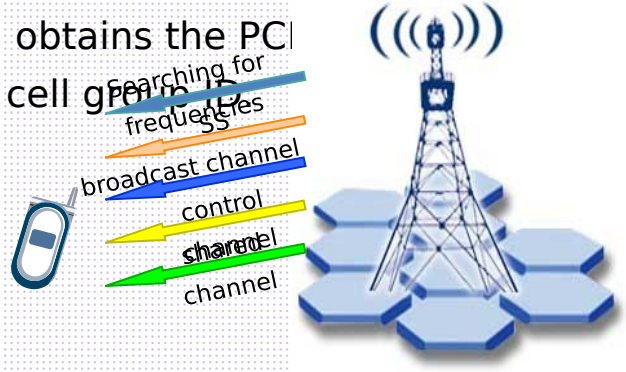
Invisible Process　Visible Process　Partially visible process

Location and Function of Cell Search



Cell search

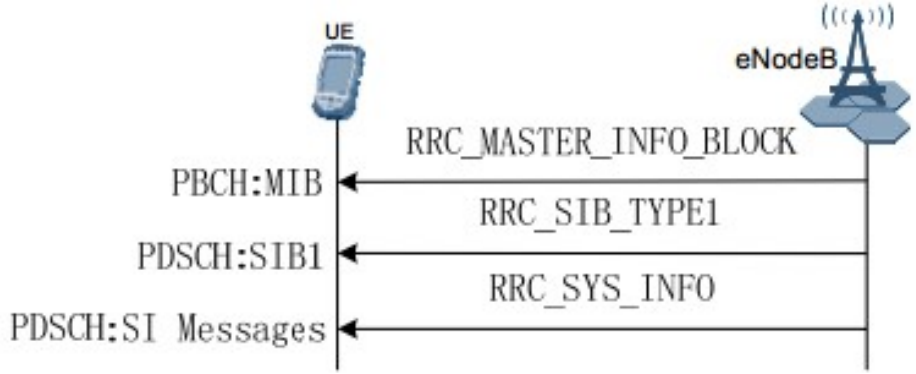
- **Basic principles of cell search**
  - Cell search is a process in which the UE implements downlink time-frequency synchronization with the E-UTRAN and obtains the serving cell ID.
  - The cell search consists of two steps.
    - Step 1: The UE demodulates the primary synchronization signal (PSS) to implement symbol synchronization and obtains the ID of the cell group
    - Step 2: The UE demodulates the SSS to implement frame synchronization, obtains the CP length and cell group ID, and obtains the PCI on the cell group's ID.



- **The complete search process of the UE from power-on is as follows:**
  - After the UE is powered on, it starts initial cell search and network search. Generally, when the UE is powered on for the first time, the UE does not know the bandwidth and frequency of the network.
  - The UE repeats the basic cell search process and traverses all frequencies in the entire spectrum to demodulate synchronization signals. This process is time-consuming, but generally does not have a strict time requirement.Some methods can be used to shorten the UE initialization time. For example, the UE stores the available network information and preferentially searches for these networks and frequencies after being powered on.
  - Once the UE finds an available network and implements time-frequency synchronization with the network to obtain the serving cell ID, that is, after the cell search is complete, the UE demodulates the downlink broadcast channel PBCH and obtains system information such as the system bandwidth and the number of transmit antennas.

Functions of each system message

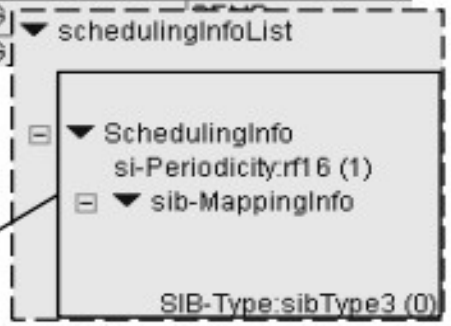
- System Information Broadcast
  - MIB: The master information block includes a limited number of most important and commonly used transmission parameters that require additional information to be obtained in the cell
  - SIB 1: Includes scheduling information of other SIBs and access information of other cells.
  - SI: The SI carries the scheduling information of the SIB instead of SIB1.
    - Cell radio configuration and other basic configuration information
    - Cell reselection information, mainly related to the serving cell
    - Intra-frequency neighboring cell list and blocklist
    - Inter-frequency neighboring cell list
    - UTRAN neighboring cell list
    - GSM neighboring cell list
    - CDMA2000 neighboring cell list
    - Home eNB Identifer
    - ETWS Notification
    - ETWS Auxiliary Notification Information
    - CMAS auxiliary notification information
    - MBMS control information



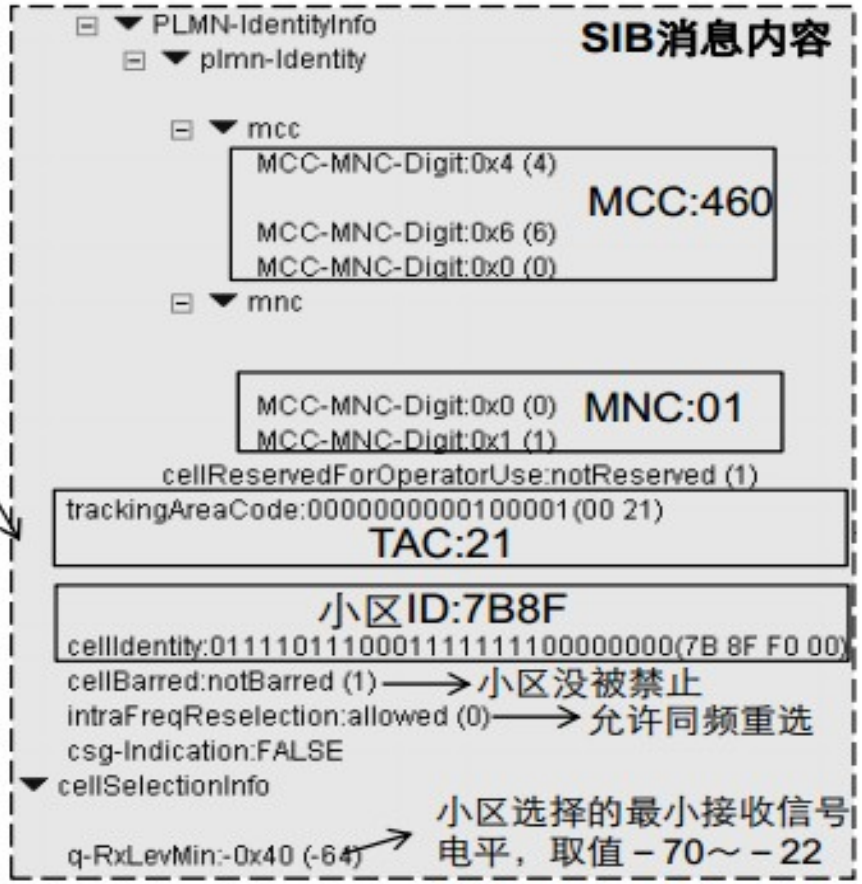
System message receiving flow instance

..	生成时间	标准接口消息类型	消息方向
1	2010-09-13 18:57:29(1874342)	RRC_MASTER_INFO_BLOCK	SEND
2	2010-09-13 18:57:29(1874555)	RRC_SIB_TYPE1	SEND
3	2010-09-13 18:57:29(1874705)	RRC_SYS_INFO	SEND
4	2010-09-13 18:58:53(3794816)	RRC_MASTER_INFO_BLOCK	SEND
5	2010-09-13 18:58:53(3795021)	RRC_SIB_TYPE1	SEND
6	2010-09-13 18:58:53(3795156)	RRC_SYS_INFO	SEND
7	2010-09-13 18:59:57(4700171)	RRC_CONN_REQ	RECEIVE
8	2010-09-13 18:59:57(4782911)	RRC_CONN_REQ	RECEIVE
9	2010-09-13 18:59:57(4786150)	RRC_CONN_SETUP	SEND
10	2010-09-13 18:59:57(4787336)	RRC_CONN_SETUP	SEND
11	2010-09-13 18:59:57(4790348)	RRC_CONN_REQ	RECEIVE
12	2010-09-13 18:59:57(4794606)	RRC_CONN_SETUP	SEND
13	2010-09-13 18:59:57(4811245)	RRC_CONN_SETUP_CMP	RECEIVE
14	2010-09-13 18:59:58(4855486)	RRC_SECUR_MODE_CMD	SEND
15	2010-09-13 18:59:58(4871342)	RRC_SECUR_MODE_CMP	RECEIVE
16	2010-09-13 18:59:58(4872023)	RRC_UE_CAP_ENQUIRY	SEND
17	2010-09-13 18:59:58(4886215)	RRC_UE_CAP_INFO	RECEIVE
18	2010-09-13 18:59:58(4903395)	RRC_CONN_RECFG	SEND
19	2010-09-13 18:59:58(4920368)	RRC_CONN_RECFG_CMP	RECEIVE
20	2010-09-13 18:59:58(4924011)	RRC_CONN_RECFG	SEND
21	2010-09-13 18:59:58(4924691)	RRC_UL_INFO_TRANSF	RECEIVE
22	2010-09-13 18:59:58(4930404)	RRC_CONN_RECFG_CMP	RECEIVE
23	2010-09-13 19:00:08(4687887)	RRC_CONN_RECFG	
24	2010-09-13 19:00:08(4702218)	RRC_CONN_RECFG	

SI消息



除了SIB1和SIB2之外其它SIB的调度信息

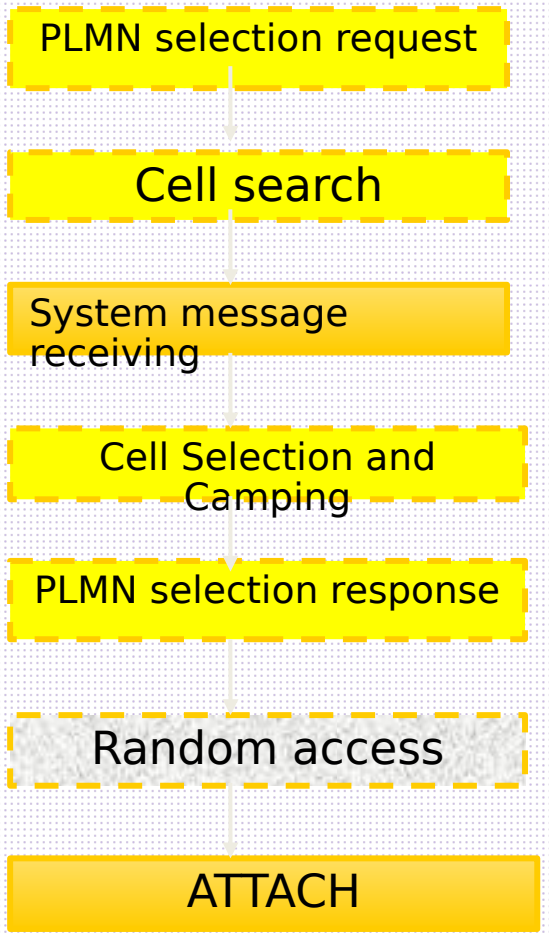


Random Access Overview

- Purpose of Random Access
  - Obtain upstream synchronization.
  - Obtaining Uplink Data Resources
- Random Access Scenario

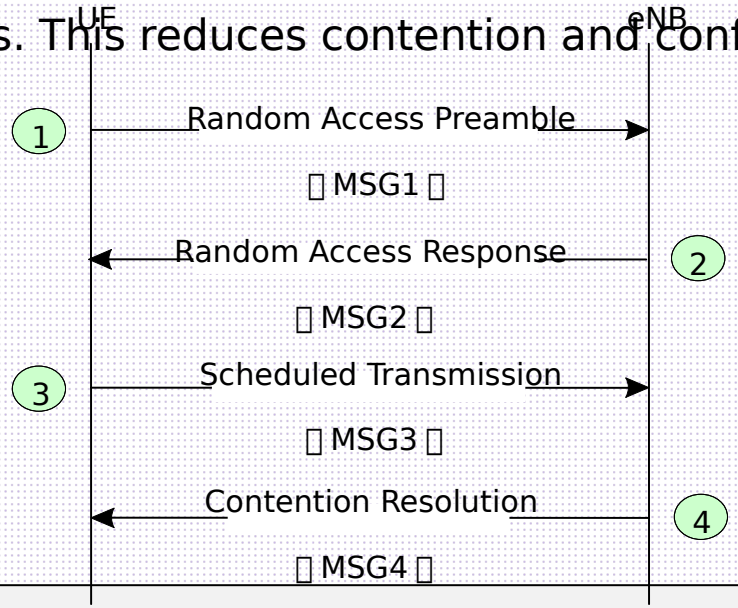
1) Initial Access from Idle Mode to Connected Mode
2) Access after radio link failure
3) Access During Handover
4) When the UE is in connected mode, uplink out-of-synchronization and downlink data arrives.
5) When the UE is in RRC_CONNECTED mode, uplink data arrives after uplink out-of-synchronization.
6) Case6：LCS：LoCation Services：Location-triggered random access.

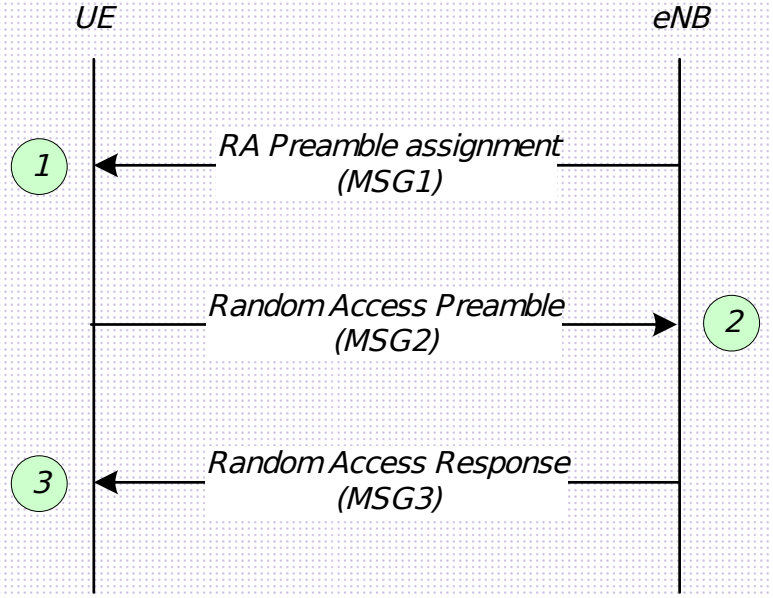
Random access is classified into contention-based random access and non-contention-based random access. Contention-based random access applies to scenarios 1, 2, and 5, and non-contention-based random access applies to



Random Access Overview

After the contention-based random access succeeds, the RRC layer of the UE generates an RRC ConnectionSetupComplete and sends the RRC ConnectionSetupComplete message to the eNodeB.The difference between non-contention-based access and contention-based access is that the eNodeB allocates access preambles. This reduces contention and conflict resolution.





contention-based random access(CBRA)

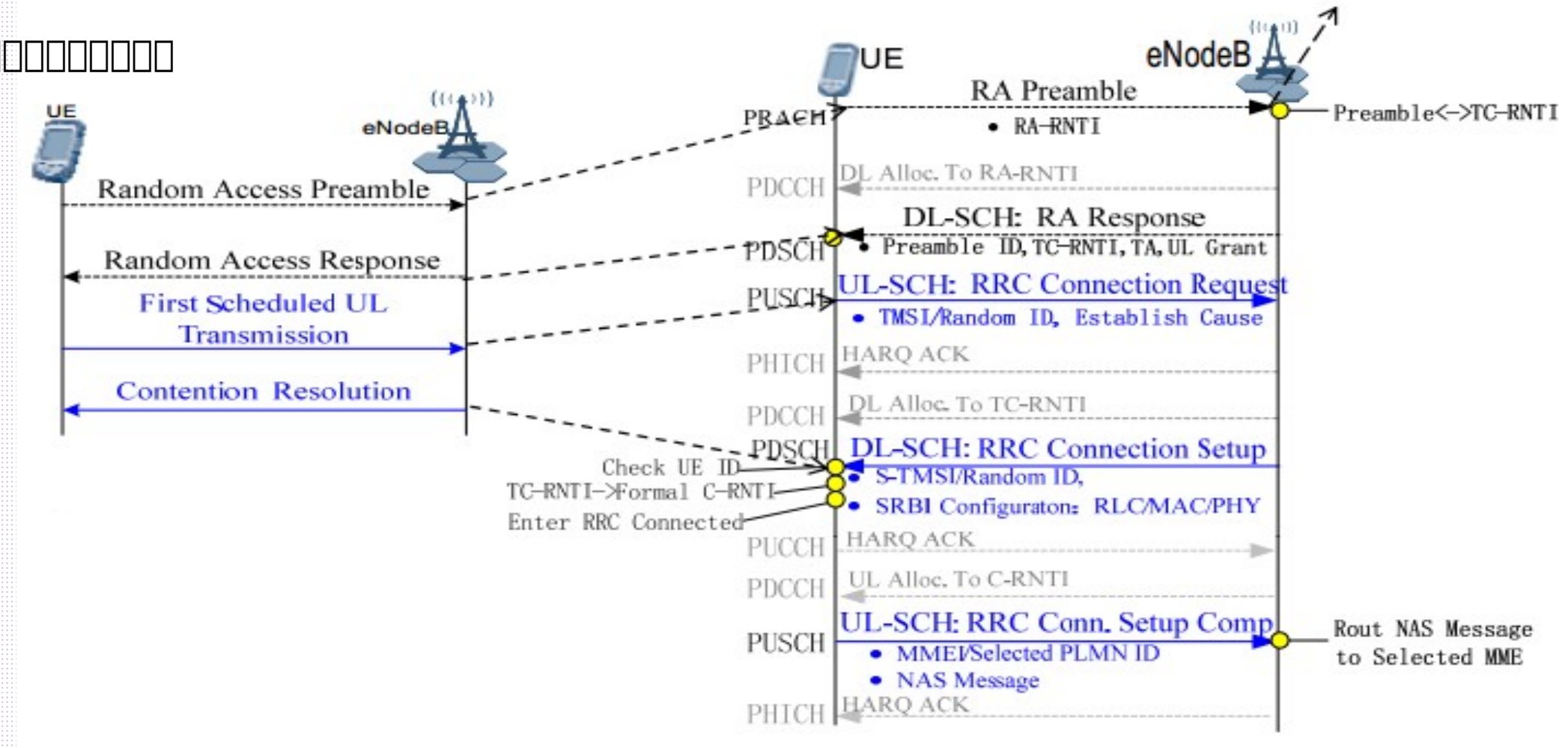
Access preambles are generated by UEs. Preambles generated by different UEs may conflict. Therefore, the eNodeB needs to contend for access of different UEs.

non-contention-based random access

The eNodeB allocates access preambles to UEs. These access preambles are dedicated preambles.In this case, no preamble collision occurs on the UE.However, when the dedicated preambles of the eNodeB are used up, non-contention-based random access becomes contention-based random access.

Random Access Signaling Procedure

□□□□□□□□□



remark：

• Solid lines are visible signaling on the LMT

•The dotted line indicates the control signaling that is invisible on the LMT

Contents

Basic Concepts of Attach Detach

- The attach procedure is that the UE sends an attach request to the CN, completes the registration of the UE with the network, and completes the establishment of the default bearer for the UE by the EPC.
- Detach is to deregister the UE on the network side and delete all EPS bearers.
- Functions of the attach procedure

- The UE registers with the EPS network.
- During network attach, a default EPS bearer is set up to provide a permanent IP connection.
- The MM context and EPS bearer context of the UE are created on the MME and UE.The EPS bearer context of the UE is created on the S-GW and P-GW.Default bearer between the UE and the P-GW; The UE can obtain the IP address allocated by the network.

Attach process

Control-plane connection establishment

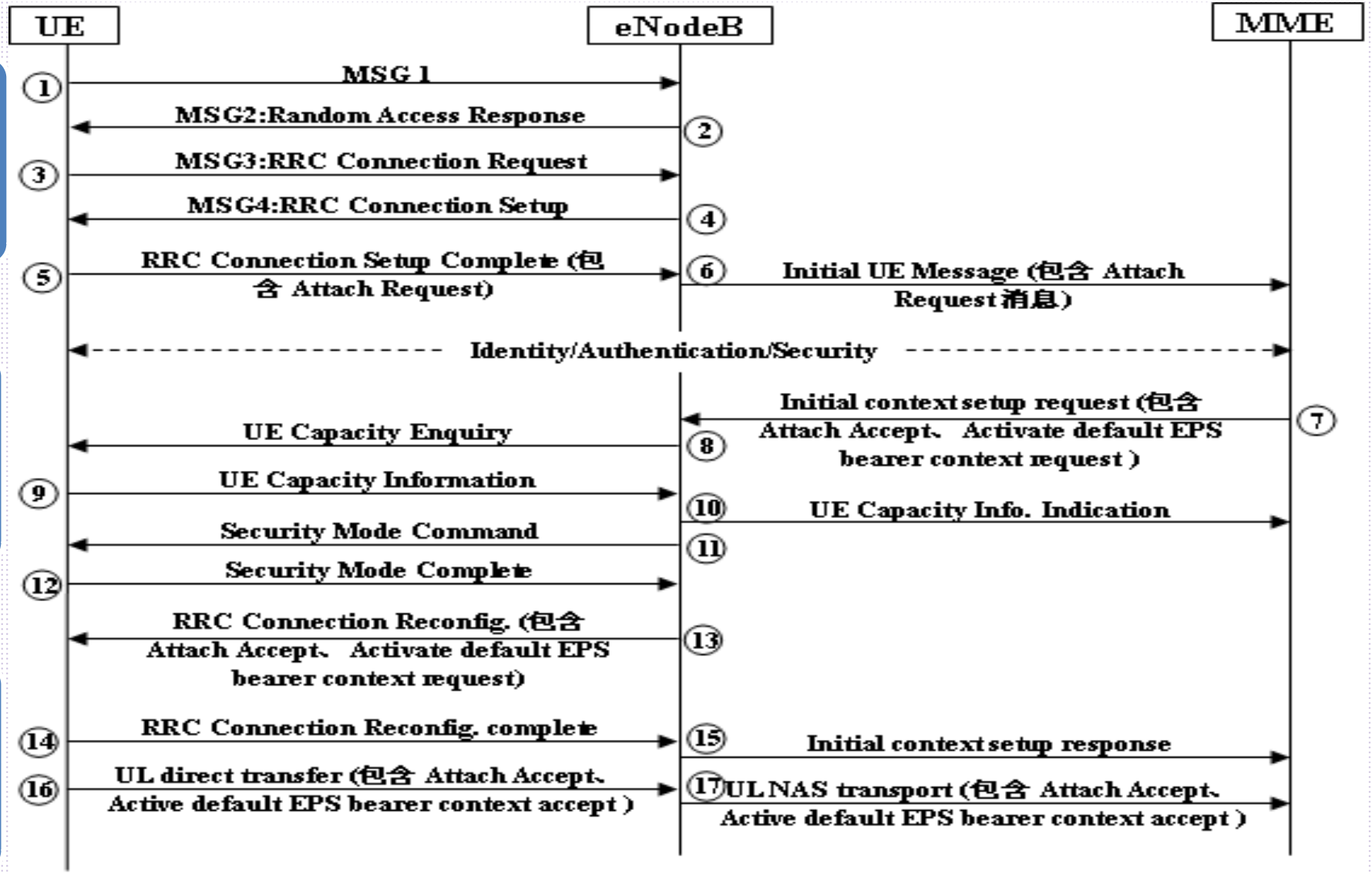
RRC connection setup and S1 signaling connection setup

Common Processes

Authentication process and security mode process

User-plane connection setup

(E-RAB setup and default bearer setup)



Description of the attach procedure

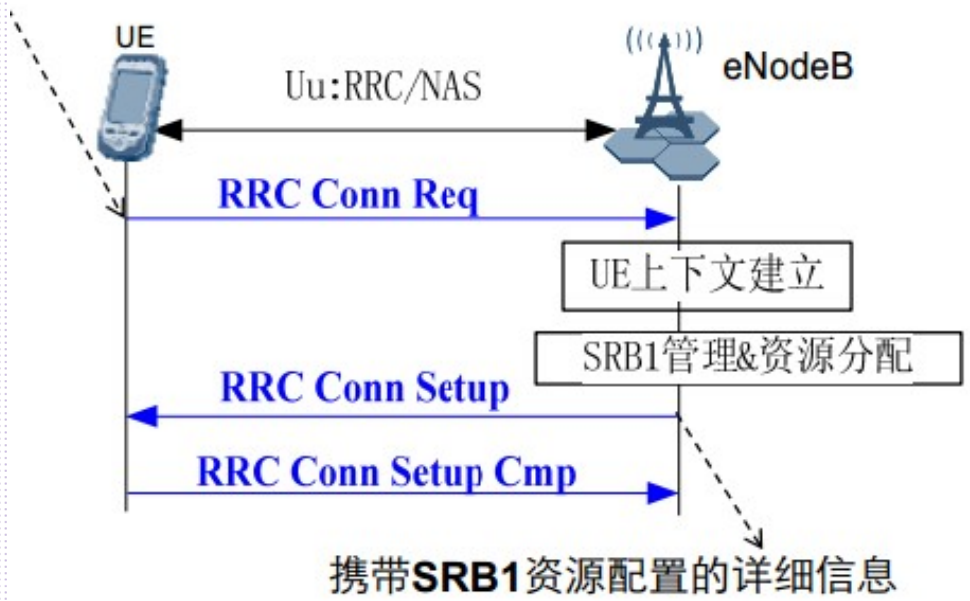
1. The UE in the RRC_IDLE state initiates a random access procedure, that is, an MSG1 message.
2. After detecting the MSG1 message, the eNB sends a random access response message, that is, the MSG2 message, to the UE.
3. After receiving the random access response, the UE adjusts the uplink transmission occasion based on the TA of Msg2 and sends an RRCConnectionRequest message to the eNodeB.
4. The eNB sends an RRCConnectionSetup message to the UE, including SRB1 bearer setup information and radio resource configuration information.
5. The UE completes SRB1 bearer and radio resource configuration and sends an RRCConnectionSetupComplete message to the eNodeB. The message contains NAS-layer Attach Request information.
6. The eNodeB selects an MME and sends an Initial UE MESSAGE message containing the NAS Attach Request message to the MME.
7. The MME sends an Initial Context Setup Request message to the eNodeB, requesting to set up a default bearer. The message includes the Attach Accept and Activate default EPS bearer context request messages at the NAS layer.
8. The eNodeB receives an Initial Context Setup Request message. If the message does not contain UE capability information, the eNodeB sends a UECapabilityEnquiry message to the UE to query the UE capability.
9. The UE sends a UECapabilityInformation message to the eNodeB to report the UE capability information.
10. The eNodeB sends a UE Capability INFO INDICATION message to the MME to update the UE capability information of the MME.
11. The eNodeB sends a SecurityModeCommand message to the UE for security activation based on the security information supported by the UE in the Initial Context Setup Request message.
12. The UE sends a SecurityModeComplete message to the eNB, indicating that the security activation is complete.
13. The eNodeB sends an RRCConnectionReconfiguration message to the UE based on the E-RAB setup information in the Initial Context SETUP REQUEST message to reconfigure UE resources, including reconfiguring SRB1 and radio resource configurations, and setting up SRB2 and DRBs (including default bearers).
14. The UE sends an RRCConnectionReconfigurationComplete message to the eNodeB, indicating that the resource configuration is complete.
15. The eNodeB sends an Initial Context Setup Response message to the MME, indicating that the UE context setup is complete.
16. The UE sends a ULInformationTransfer message to the eNodeB. The message contains the Attach Complete and Activate default EPS bearer context accept messages at the NAS layer.
17. The eNodeB sends an uplink direct transfer UPLINK NAS Transport message to the MME. The message contains the Attach Complete and Activate default EPS bearer context accept messages at the NAS layer.

Contents

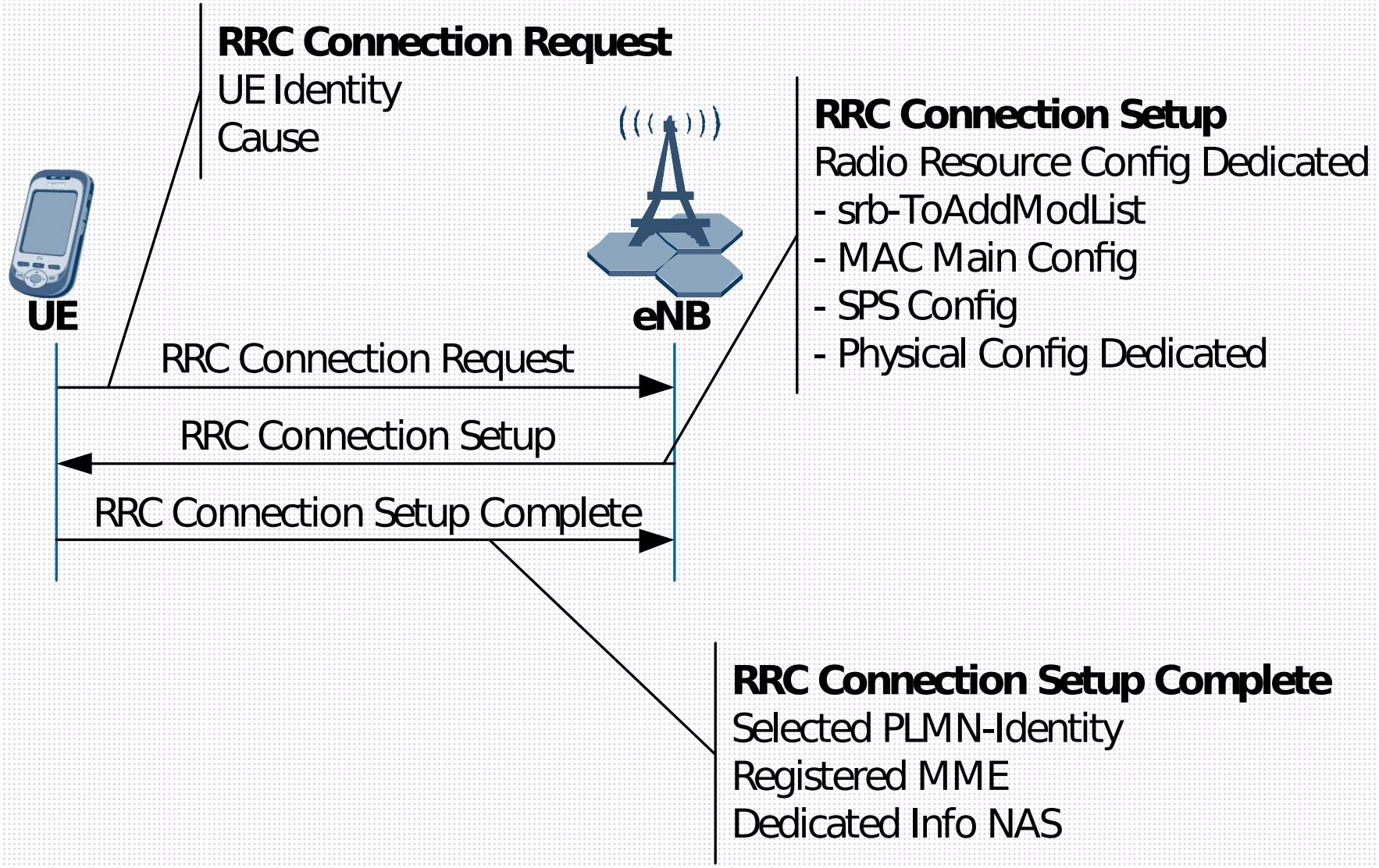
Overview of RRC Connection Setup

- RRC connection setup is a process of setting up SRB1.
- The RRC connection setup cause value is determined by the NAS procedure type. Different NAS procedures correspond to different RRC connection setup causes.

NAS process	RRC Connection Setup Cause	call type
Attach	MO-signalling	originating signalling
TAU	MO-signalling	originating signalling
Detach	MO-signalling	originating signalling
Service Request	MO-data，Request to set up service bearer radio resources，	originating calls
	MO-data，Uplink signaling request resource，	originating calls
	MT-access， Responding to paging，	terminating calls
Extended Service Request	MO-data， mobile originating CSFB，	originating calls
	MT-access， mobile terminating CSFB，	terminating calls
	Emergency，mobile originating CSFB emergency call，	emergency calls

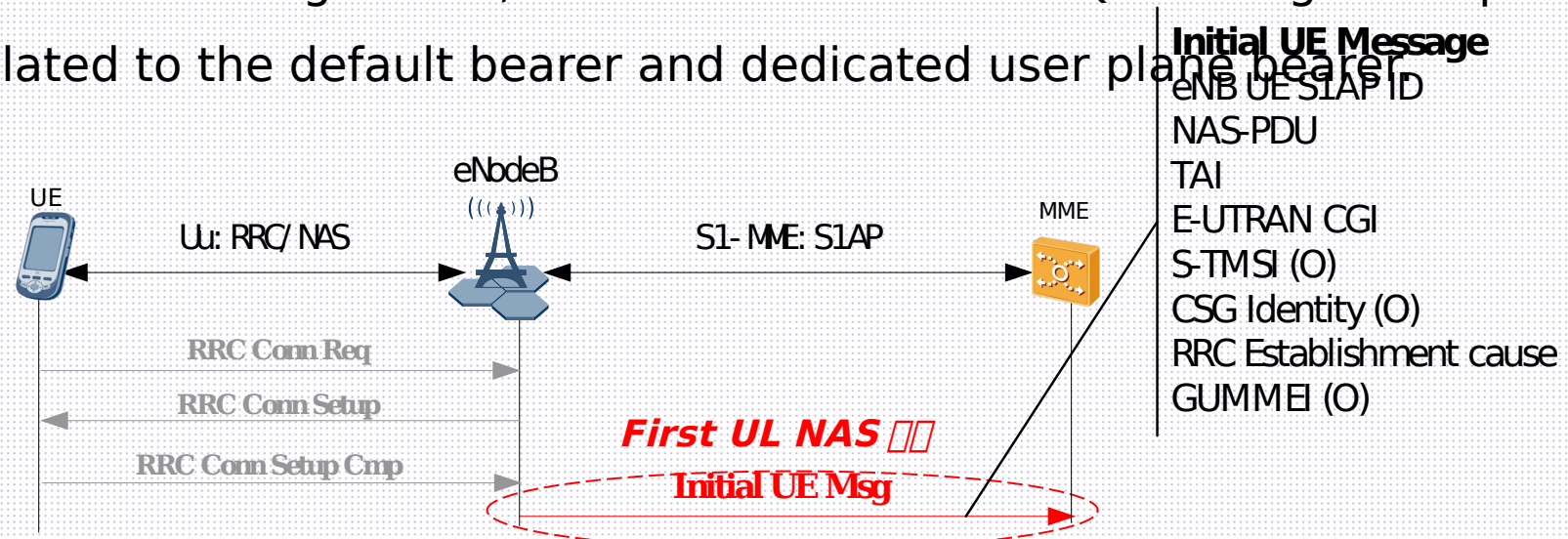


Signaling procedure and key parameters for RRC connection setup



Initial UE Message

- After an RRC connection is set up, the eNodeB receives an RRC Connection Setup Complete message carrying the first uplink NAS message. The eNodeB activates the NAS transmission process and sends the first uplink NAS message to the MME in an Initial UE MESSAGE message. The S1 signaling connection is set up.
- The Initial UE MESSAGE message carries the following information:
  - EMM：EPS Mobility Management,"ATTACH REQ" message：the protocol processes signaling related to UE mobility and different ciphering procedures.
  - ESM：EPS Session Management ,"PDN CONNECTIVITY REQ"message. The protocol processes signaling related to the default bearer and dedicated user plane bearer.

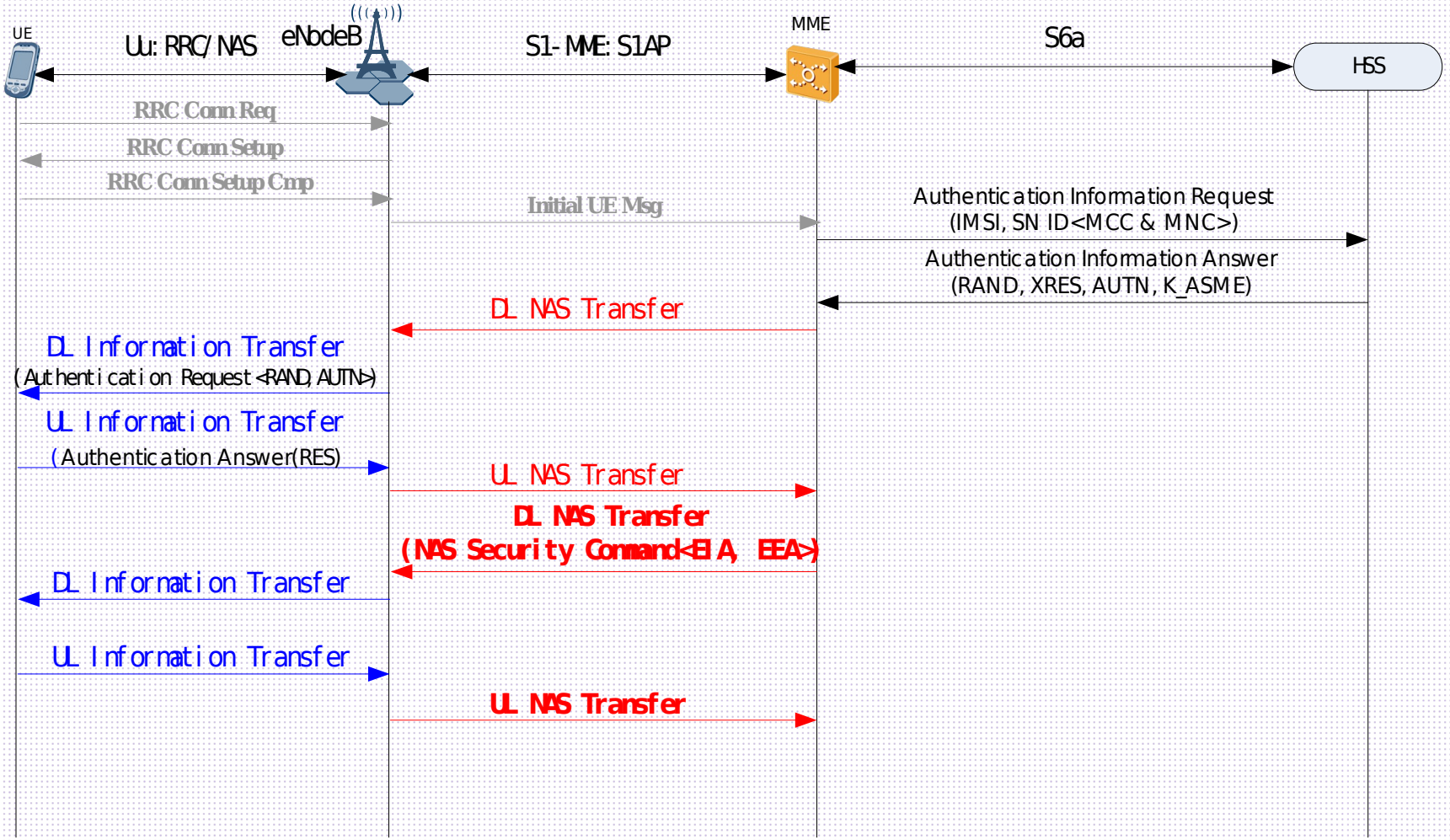


Authentication and NAS Encryption Process

- The NAS process is an interaction process between the core network and the UE, including authentication and encryption.

a. The authentication process is used to derive a new set of keys.
b. The security mode process is used to make the security context generated based on the new key take effect.
c. In processes such as identity, the core network obtains related information from the UE.

The NAS process is represented as uplink and downlink direct transmission messages for the eNodeB.

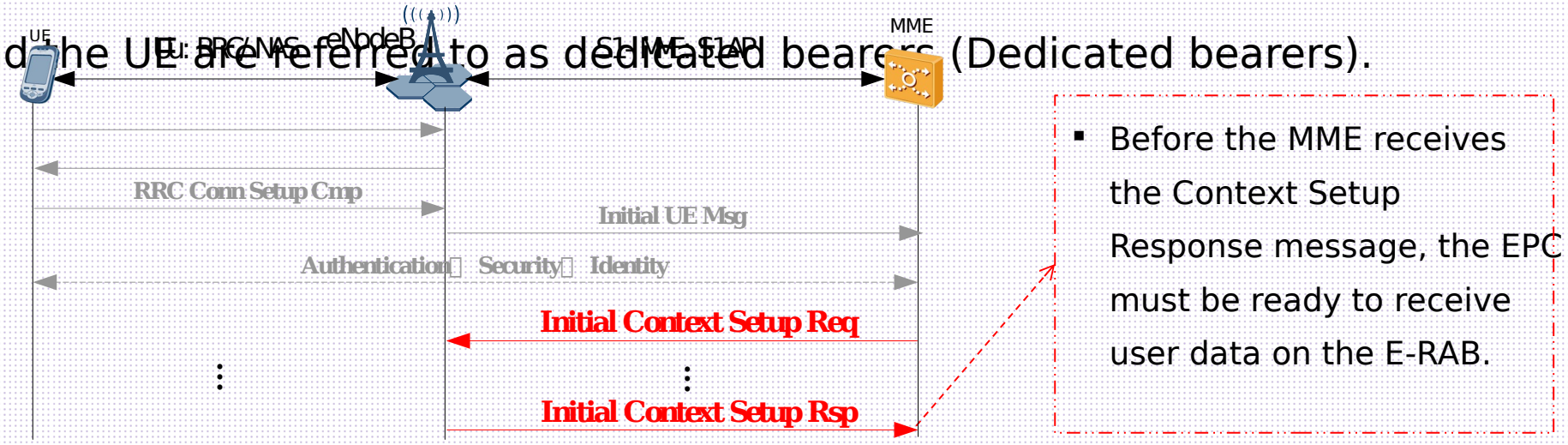


Uplink Information Transmission Procedure

- function
- This signaling is intended to transfer NAS or (tunneled) non-3GPP indication information from the UE to the E-UTRAN. That is, the NAS information needs to be transmitted is nested in this message.
- When NAS or non-3GPP indication information needs to be transmitted, the UE initiates the uplink information transmission process by sending a UL Information Transfer message.
- NAS signaling transmission aims to transmit UE-MME signaling over the S1 interface.The NAS signaling is carried in an IE in the Initial UE MESSAGE, DOWNLINK NAS TRANSPORT, or UPLINK NAS TRANSPORT message.

Initial context setup procedure

- After the UE initiates an initial context setup request on the access network side, the core network requests the initial context setup.
- The initial setup procedure establishes a default bearer for the UE. According to 3GPP TS 23.401, when the UE accesses the PDN for the first time, the EPC needs to allocate the first bearer to the UE, and the bearer remains. The UE is disconnected from the PDN. This bearer is called the default bearer.
- In contrast, after the default bearer is established, other bearers established between the same PDN and the UE are referred to as dedicated bearers (Dedicated bearers).



- Before the MME receives the Context Setup Response message, the EPC must be ready to receive user data on the E-RAB.

Process of querying UE capabilities

- When a UE attaches to the network, the S1AP_INITIAL_CONTEXT_SETUP_REQ message sent by the EPC does not contain the UE capability. Instead, the eNodeB initiates a query request to the UE, and the UE reports the request to the eNodeB. In addition, the eNodeB reports the UE capability indication information to the EPC through the S1 interface.
- During the idle-to-active procedure, the EPC sends the UE capability to the eNodeB through the S1AP_INITIAL_CONTEXT_SETUP_REQ. The eNodeB does not need to query the UE, saving air interface resources.

Example of the UE capability query procedure

```
struDL-DCCH-Message
  message
    c1
      ueCapabilityEnquiry
        rrc-TransactionIdentifier: ---- 0x2(2) ---- *****10*
        criticalExtensions
          c1
            ueCapabilityEnquiry-r8
              ue-CapabilityRequest
                RAT-Type: ---- eutra(0) ---- ******00,00******
                RAT-Type: ---- utra(1) ---- **0001**
                RAT-Type: ---- geran-cs(2) ---- ******00,10******
                RAT-Type: ---- geran-ps(3) ---- **0011**
                RAT-Type: ---- cdma2000-1XRTT(4) ---- ******01,00******
```

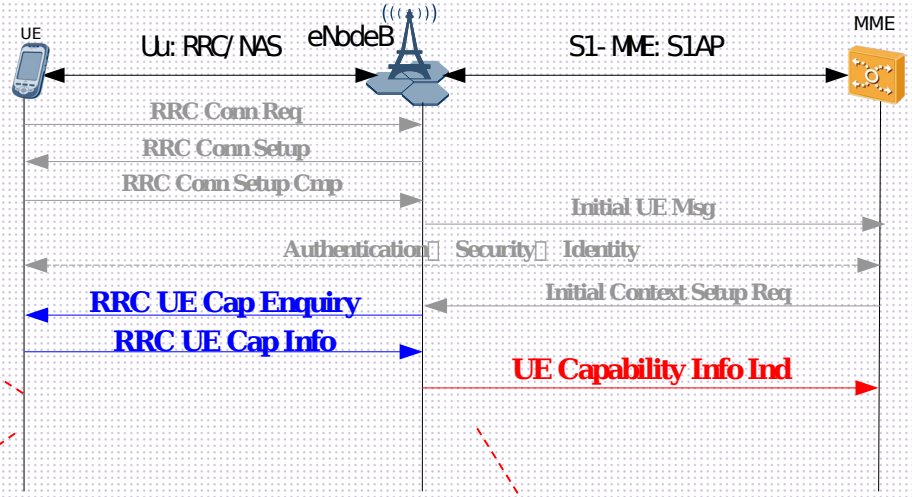
Whether LTE is supported?

```
UE-CapabilityRAT-Container
  rat-Type: ---- eutra(0) ---- 0000****
  ueCapabilityRAT-Container
    ueEutraCap
      UE-EUTRA-Capability
        accessStratumRelease: ---- rel9(1) --
        ue-Category: ---- 0x5(5) ---- **100***
        pdcp-Parameters
        phyLayerParameters
        rf-Parameters
        measParameters
        featureGroupIndicators: ---- '0111111
        interRAT-Parameters: ---- (0) ---- *000
```

The feedback 0 indicates that LTE is supported.

The UE type is 5.

UE Support for Automatic Neighbor Relationship (ANR)

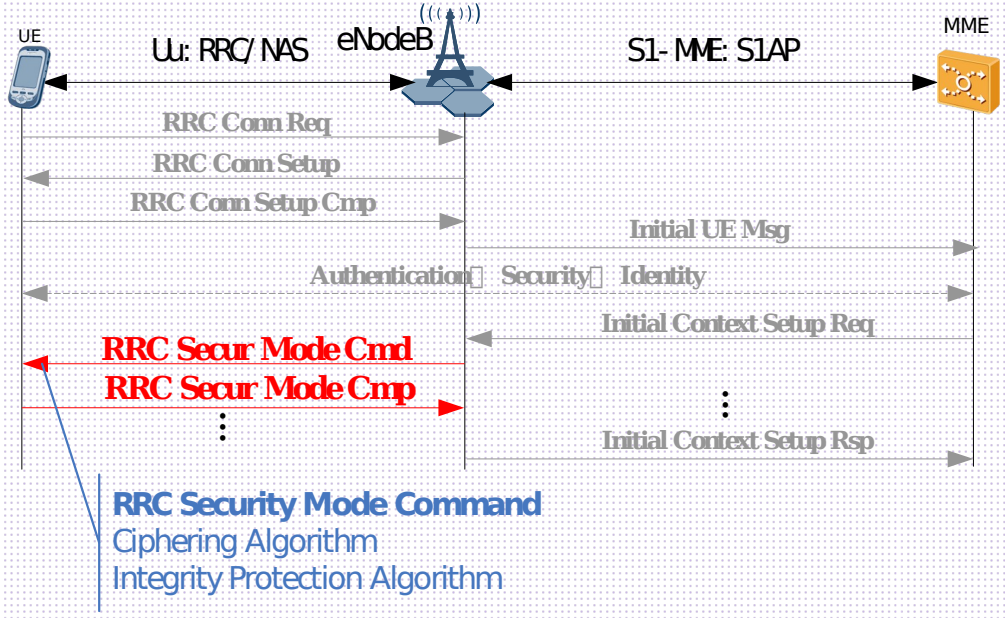


After receiving the UE capability message, the MME replaces the previously stored UE capability information.

AS Security Mode Process

- Purpose:
- The security mode procedure is used to activate ciphering and integrity protection at the access stratum. Only after the AS security function is activated, a radio bearer other than SRB1 can be set up in the RRC Connection Reconfiguration message.
  - Start time:
  - After SRB1 is set up and before SRB2 is set up

- For integrity protection, the secure mode command and the secure mode complete message are initiated themselves, and for encryption, the next message in the secure mode process is initiated.
- Integrity protection applies only to signaling-plane SRBs. Encryption applies to signaling-plane SRBs and user-plane DRBs.



RRC Connection Reconfiguration Procedure

- In this procedure, the UE configures SRB2 and DRB for the default bearer based on the RRC reconfiguration message delivered by the eNodeB and reports an RRC reconfiguration complete message to the eNodeB.
  - RRC connection reconfiguration functions:

1. Establish, modify, or release a radio bearer.

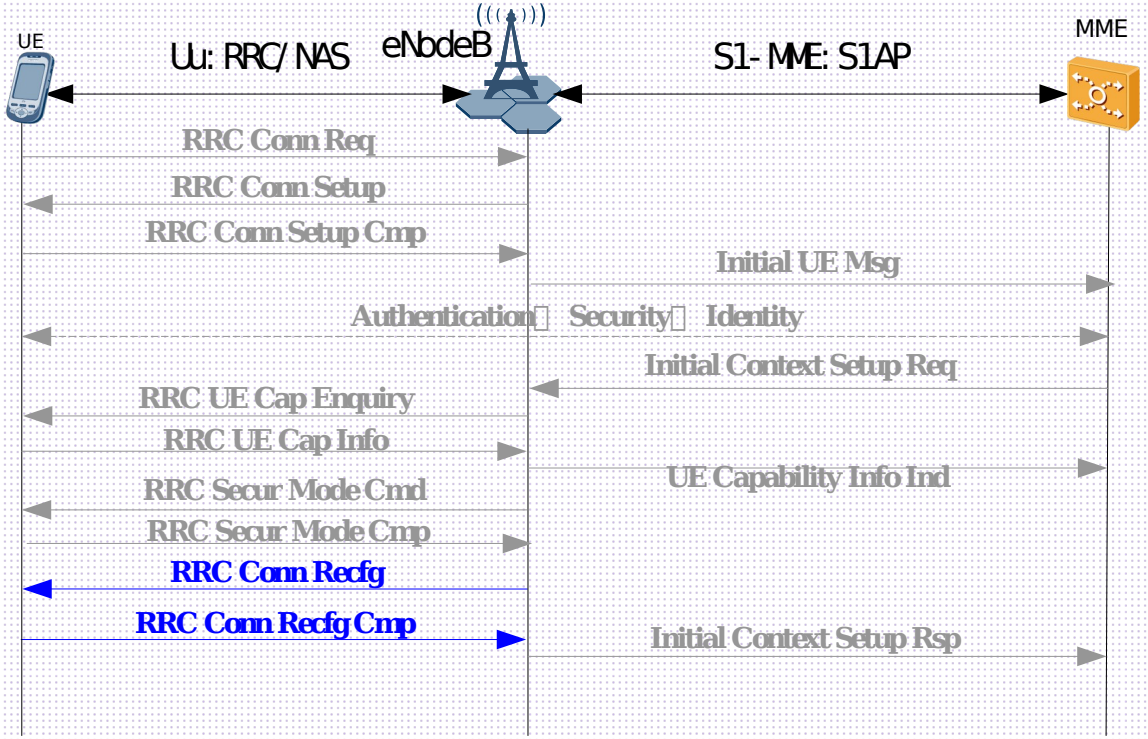
   IE: radio Resource Config

2. Perform the handover.

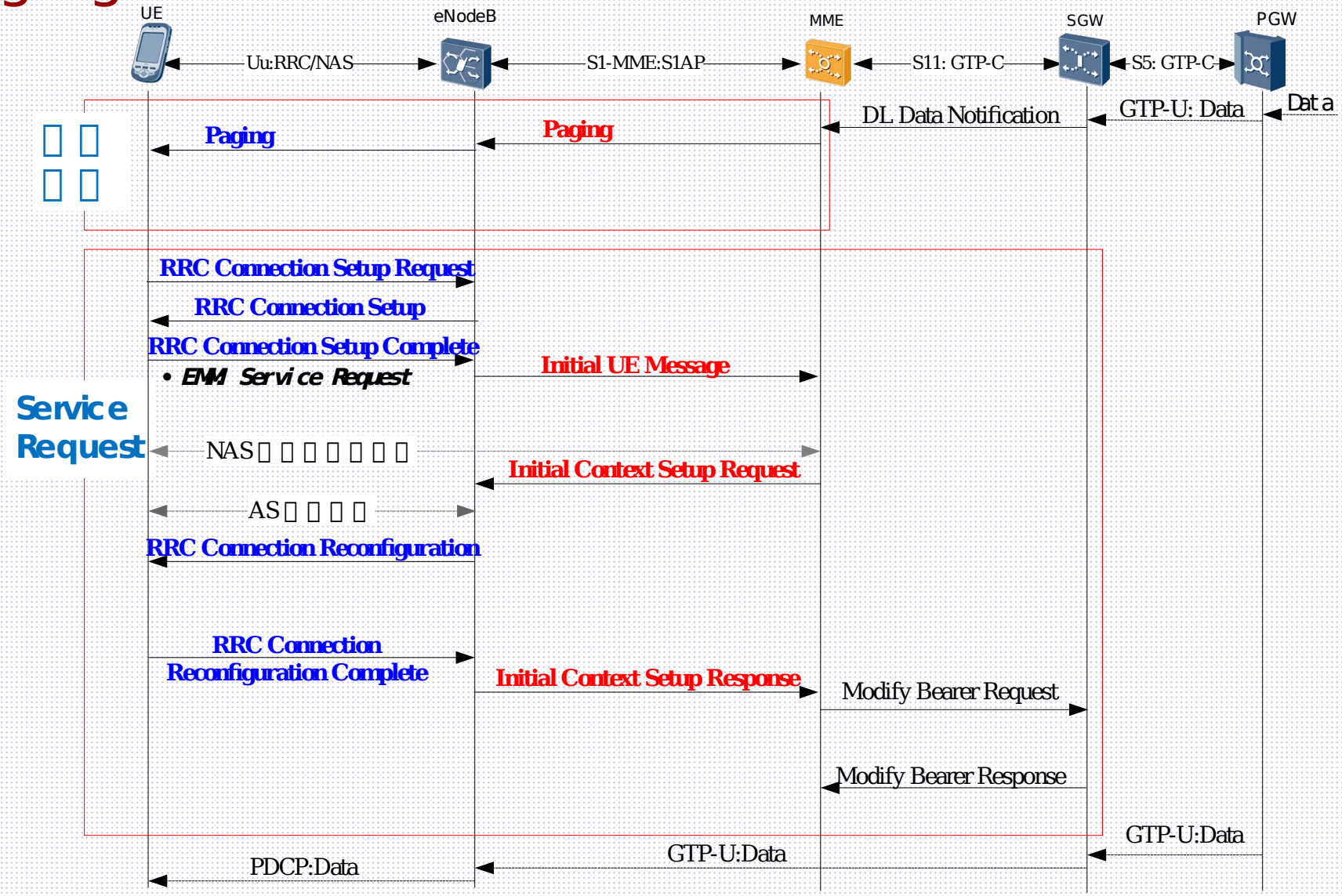
   IE: mobility ControlInformation

3. Create, change, or release measurement configurations.

   IE: meas Config



Paging Procedure



Thank You

www.huawei.com